Table of Contents

M Evaluation Factors for Award

M.1 General Information

Proposals shall be prepared in accordance with and comply with the requirements and instructions contained in this Request for Proposal (RFP). Each proposal will be evaluated against the evaluation factors identified herein. The details on the complete evaluation process are outlined in M.2, Evaluation Process.

M.2 Evaluation Process

In accordance with Federal Acquisition Regulation (FAR) 15.202 and as described herein, a multi-phased approach will be used to determine the overall best value to the Government for this acquisition. Each proposal will be reviewed and evaluated in accordance with its contents; the Government will make no assumptions related to the Offeror's performance that the Offeror does not specify in its proposal.

In light of the First Responder Network Authority's (FirstNet) objective-based acquisition approach and the unique nature of the FirstNet program and the Middle Class Tax Relief and Job Creation Act of 2012 (the Act), the Government will consider unique, innovative approaches to achieving an overall best value solution consistent with the objectives as set forth in Section C, Statement of Objectives (SOO) and the requirements and recommendations specified in Section J, Attachment J-3, FCC TAB RMTR. The Government will consider any and all proposed solutions utilizing emerging technologies and/or non-traditional practices or solutions with regard to the overall Nationwide Public Safety Broadband Network (NPSBN) in accordance with the terms and conditions, instructions, and evaluation criteria as stated herein.

Any exceptions or deviations by the Offeror to the terms and conditions stated in the Offeror's proposal for inclusion in the resulting contract may make the offer unacceptable for award without discussions. If an Offeror proposes exceptions to the terms and conditions of this RFP, the Government may make an award, without discussions, to another Offeror that did not take exception to the terms and conditions, if such Offeror is determined to be the best overall value for this effort.

As part of the multi-phased approach, the Government reserves the right to request Offerors to conduct oral presentations and/or technical demonstrations as a result of this RFP. Those Offerors will be notified and provided any additional information and instructions, as necessary, regarding oral presentations and/or technical demonstrations.

The Day 1 task order evaluations will *not* be conducted separately from the evaluation of the overall NPSBN proposed solution as they make up specific portions of the NPSBN solution, based on the SOO (Section C) and associated attachments in Section J.

M.2.1 Phase I – Capability Statements

For Phase I of the multi-phased approach, interested parties should demonstrate they are capable of performing the work by providing a capability statement (see FAR Part 15.202 and Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.2.4, Submission of Capability Statements, for instructions). Following review and evaluation of all capability statements received as a result of this phase, those deemed best qualified based on the evaluation criteria stated herein will be

invited to submit a proposal in accordance with the instructions contained in Section L, Instructions, Conditions, and Notices to Offerors or Respondents.

Notifications will be issued to *all* Offerors that submit a capability statement as a result of this RFP. Each notification will include feedback regarding evaluation of the capability statement that identifies strengths and/or weaknesses that shows whether the company is or is not, based on the capability statement review and evaluations, considered a viable competitor.

Capability statements will be evaluated based on the following criteria, which are of equal importance:

- **Public safety use and adoption of the NPSBN** – Offerors will be evaluated based on their demonstration of their ability to successfully drive adoption and use of the NPSBN by public safety users.
- **Nationwide coverage and capacity** – Offerors will be evaluated based on their demonstration of their ability to provide Band 14 and non-Band 14 coverage and capacity in each of the 56 states and territories, including rural and non-rural areas.
- **Rural partnerships** – Offerors will be evaluated based on their demonstration of their existing and planned partnerships with rural telecommunications providers, including commercial mobile providers, utilizing existing infrastructure to the maximum extent economically desirable to speed deployment in rural areas.
- **Ability to monetize network capacity** – Offerors will be evaluated based on their strategy and demonstration of their ability to monetize network capacity, which may include a secondary user customer base and sales/distribution channels to reach primary and secondary users.
- **Financial sustainability** – Offerors will be evaluated based on their demonstrated approach and financial sustainability. Additionally, Offerors' financial stability will be evaluated in regard to their ability to develop, implement, sustain, and enhance the NPSBN based on the Initial Operational Capability (IOC)/Final Operational Capability (FOC) milestones set out in Section J, Attachment J-8, IOC/FOC Target Timeline.

M.2.2 Phase II – Solicitation Conformance

During this phase, the Government will conduct an initial review of the proposals received in order to verify conformance and completeness with the RFP instructions, including any/all attachments and exhibits, prior to commencement of evaluations as stated herein in Section M.2.3, Phase III – Pass/Fail, and Section M.2.4, Phase IV – Detailed Evaluation.

This conformity review will consist of verification that all documentation has been provided in accordance with Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3, Proposal Format and Submission Instructions. The Government will also utilize the Section J, Attachment J-22, Solicitation Conformance Traceability Matrix (SCTM), in order to make a determination regarding completeness.

Failure to submit any information and/or documentation as stated in this RFP and as listed on the SCTM may result in the proposal submission being removed from any further consideration.

M.2.3 Phase III – Pass/Fail

During this phase, the Government will review and evaluate each proposal to ensure it meets the pass/fail factors identified herein. The following pass/fail factors will be evaluated based on the criteria

as stated herein. Failure to pass any of these factors may result in the proposal submission being removed from any further consideration.

M.2.3.1 FirstNet Minimum Payment Thresholds

Offerors must propose payments to FirstNet to be disbursed on an annual basis. The Offeror's proposed solution must demonstrate its ability to sustain the annual payments to FirstNet for the life of the contract, no less than the minimum payment thresholds described in Section B, Supplies or Services and Prices/Costs, Section B.4.4, FirstNet Operational Sustainability. Payments to FirstNet must be submitted for each of the 56 states and territories. For this phase, the Offeror must demonstrate its ability to meet the minimum payment thresholds. The minimum payment is evaluated based on the sum of the payments proposed for all 56 states and territories for each contract year without regard to the Net Present Value (NPV) calculation (see Section M.4.5.1, Net Present Value of Payments to FirstNet).

M.2.3.2 Rural Partners and Subcontractors

Offerors shall complete Section J, Attachment J-2, Nationwide and Rural Coverage Compliance Checklist, to demonstrate their ability to meet the objective to provide coverage in each of the 56 states and territories and to ensure that rural coverage includes partnerships with rural telecommunications providers. The Offeror's solution must demonstrate commitment to exercise rural telecommunications provider partnerships for at least 15 percent of the total rural coverage area nationwide at FOC. While Attachment J-2 requests these data by states, the 15 percent coverage factor will be evaluated on a nationwide basis only for this phase.

M.2.4 Phase IV – Detailed Evaluation

Those Offerors whose proposed solutions have been determined to conform to the RFP in Phase II and successfully pass Phase III will move into Phase IV. During this phase, the Government will commence the detailed evaluation of all information and documentation received from the Offerors based on the evaluation factors as stated herein.

The Government may consider, as part of its evaluation, any oral presentations and/or technical demonstrations or other discussions and publicly available materials gathered as part of the Government's evaluation. All of these materials may be used as part of the evaluation of the Offeror's ability to meet the objectives stated in Section C, SOO.

M.3 Basis for Award

Contract award shall be made to the responsible Offeror whose offer, in conforming to this RFP, provides the overall best value to the Government, when all evaluation factors are considered. All evaluation factors, when combined, are significantly more important than the value proposition. The Government may conduct a trade-off analysis and make an award to other than the highest technically rated Offeror or other than the Offeror presenting the most favorable value proposition. Due to the unique nature of FirstNet and the NPSBN, rather than conduct a *traditional* trade-off analysis where the Government typically considers price and non-price factors, the trade-off analysis for this acquisition will utilize the results of a value proposition assessment (see Section M.4.5) and non-price factors to determine the overall best value solution.

The Government reserves the right to *not* make an award as a result of this competition if, in the opinion of the Government, none of the submissions would provide satisfactory performance that is

considered fair and reasonable and/or economically feasible in the Government's sole determination. Additionally, the Government reserves the right to remove an Offeror's proposed solution from further consideration if it is determined to be unacceptable in any of the evaluation factors and/or sub-factors.

M.4 Evaluation Factors

The evaluation will consist of a determination and analysis of strengths, weaknesses, and risks of each proposed solution. Risk will be included in the evaluation of each factor (and/or sub-factors) and will not be evaluated as a separate factor. The Government may consider all proposal information submitted when assessing risk. The Offeror will be evaluated based on its demonstration and understanding of the objectives, including demonstrated creativity and thoroughness in its proposed solution. The Government may consider all proposal information submitted and presented pertaining to the Offeror's proposed solution when conducting the evaluation and determining overall best value.

The following evaluation factors will be utilized in order to determine which Offeror provides the best overall value. Evaluation factors are comprised of Business Management (Section M.4.1), Coverage and Capacity (Section M.4.2), Products and Architecture (Section M.4.3), the Offeror's Past Performance (Section M.4.4), and the Offeror's Value Proposition Assessment (Section M.4.5).

Evaluation factors are listed in descending order of importance:

- Business Management is more important than Coverage and Capacity.
- Coverage and Capacity and Products and Architecture are of equal importance.
- Business Management, Coverage and Capacity, and Products and Architecture combined are more important than the Volume III – Offeror's Value Proposition Assessment.
- The Volume III – Offeror's Value Proposition Assessment is more important than Past Performance.

Sub-factors for any of the evaluation factors are of equal importance unless otherwise stated.

M.4.1 Volume I – Business Management Factor

The Offeror will be evaluated based on its understanding of the effort, including innovation, creativity, and thoroughness shown in addressing the objectives (Section C, SOO) and applicable Section J attachments. The Government will evaluate the Offeror's business management approach to providing effective management of its delivery, operation, and maintenance of the NPSBN. The proposed approach will be evaluated to determine the extent to which it demonstrates a comprehensive, sound, efficient, and realistic approach to managing and ensuring successful contract performance within time and budget constraints.

The Business Management Factor includes evaluation in the following sub-factors:

- General
- Leadership and program management
- Public safety customer acquisition
- Customer care and life-cycle sustainment
- Offeror financial sustainability
- Delivery mechanism for state plans
- Quality Assurance Surveillance Plan
- Deliverables table

M.4.1.1 Section One – General

The Offeror's proposed solution will be evaluated based on the following elements:

- Small business subcontracting plan – This shall be evaluated pursuant to FAR Part 19.705.
- Contractor responsibility information – This shall be evaluated pursuant to FAR 9.104 in order to determine a prospective Contractor's determination of responsibility.
- Past performance – This shall be evaluated in accordance with Section M.4.4, Past Performance Factor.
- Offeror's experience – This shall be evaluated based on any proposed experience with regard to the Offeror's solution for the NPSBN to include the Offeror's proposed structure and experience of the subcontractors/teaming partners, the relationship between the Offeror and these organizations, and their combined ability to support the proposed solution with innovative approaches.

M.4.1.2 Section Two – Leadership and Program Management

The Offeror's solution must demonstrate its ability and proposed approach regarding leadership and program management. This will be evaluated based on the Offeror's proposed management plan and approach to achieving its stated solution, which demonstrates the following elements:

- Solution to ensure the services meet objectives in Section C, SOO
- Overall staffing plan for the NPSBN, including any proposed teaming arrangements and/or subcontractors
- Integrated Master Schedule and Work Breakdown Structure that encompass build-out and transition-to-operations activities with respect to the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline
- Details of existing 3rd Generation Partnership Project (3GPP) standards-based mobile broadband service capabilities, mobile and fixed broadband infrastructure, and operations controlled or managed by the Offeror or its proposed teaming partners and/or subcontractors
- Solution to leverage existing commercial and/or other infrastructure

The Offeror's proposed solution will also be evaluated based on its approach pertaining to:

- Corporate-level organizational structure, including the teaming/subcontracting roles and responsibilities as they relate to the NPSBN
- Comprehensive program management reflecting the Offeror's ability to provide seamless, efficient management of the NPSBN over the life of the contract and any subsequent task orders
- Supporting and facilitating FirstNet's compliance with the Act and other applicable local, state, tribal, and federal legislation (including, for example, the National Environmental Policy Act [NEPA], and the Communications Act)
- Organizational structure, staffing plan, and qualifications and experience of key personnel and executive leadership that will support the FirstNet program

M.4.1.3 Section Three – Public Safety Customer Acquisition

The Offeror must propose an approach to satisfy FirstNet's public safety customer acquisition objectives. This sub-factor will evaluate the Offeror's proposed public safety device connection targets (connection targets), which represent its anticipated number of public safety device connections

(primary users and extended primary users) by each of the 56 states and territories over the life of the contract, as detailed in Section L, Instructions, Conditions, and Notices to Offerors or Respondents. The Offeror's proposed connection targets will be evaluated relative to the estimated current demand at a state and territory level for the primary user group, as well as the extended primary user group as identified in Section J, Attachment J-24, Public Safety Device Connections Template.

This sub-factor will also evaluate the Offeror's proposed strategy to minimize time required to provide broadband services to public safety. This includes the Offeror's current sales and marketing structure, proposed go-to-market strategy for adoption, and nationwide sales and marketing plan to drive widespread adoption of FirstNet priority- and preemption-capable products and services by public safety users. Preference in the evaluation will be placed on adoption by primary users.

The Offeror's proposed solution will be evaluated based on its approach pertaining to:

- Connection targets
- Go-to-market strategy to sell and market services, including priority and preemption, to public safety users, including pricing and incentive programs
- Marketing of an applications ecosystem
- Description and staffing of the marketing and sales organization(s) tasked to support the NPSBN, including the proposed strategy and approach to ensure strategic alignment and mitigation of sales and marketing channel conflict among teaming partners to ensure adoption and use of the NPSBN
- Ability to meet current, emerging, and future customer needs and standards, including a device portfolio and estimated price points

M.4.1.4 Section Four – Customer Care and Life-Cycle Sustainment

The Offeror's proposed approach must demonstrate its ability to satisfy customer care and life-cycle innovation as stated in Section C, SOO. This sub-factor will be evaluated based on the Offeror's proposed ability to demonstrate that its solution will deliver provisioning capabilities, and solution for service and delivery, including all linkages to sales, fulfillment, and customer care. Additionally, the Offeror's solution will be evaluated based on the proposed billing management capabilities and proposed management approach.

The Offeror's proposed solution will be evaluated based on its approach pertaining to:

- Performance monitoring and reporting for devices/network equipment, services, and customer care, including providing subscribers with activation, repair, technical assistance, replacement devices, and emergency restoration support
- Metrics to monitor customer satisfaction, the service levels reported by current customers, and the solution for maintaining or improving these service levels over the 25-year period of performance
- Customer care strategy to minimize churn and promote customer retention among public safety users
- Current billing support services for broadband and wireless services and any current public safety services throughout the FirstNet service area

M.4.1.5 Section Five – Offeror Financial Sustainability

The Offeror's proposed approach must demonstrate its ability to satisfy financial sustainability requirements. This section will be evaluated based on the Offeror's solution regarding its financial robustness to develop, implement, sustain, and enhance the NPSBN within the time frames, duration, and objectives set out in this RFP.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

The Offeror's proposed solution will be evaluated based on the following aspects:

- Financial statements of the Offeror in order to demonstrate financial stability and capacity
- Details of source funding or financing to support the NPSBN
- Terms of any parent company or other guarantees
- Financial forecasts and how the Offeror proposes to commercialize the excess network capacity

M.4.1.6 Section Six – Delivery Mechanism for State Plans

In accordance with the Middle Class Tax Relief and Job Creation Act of 2012 (the Act), upon completion of the RFP process, FirstNet must present a plan to the governor of each state and territory that includes, among other things, "… details of the proposed plan for buildout of the nationwide interoperable, broadband network in such State."

It is FirstNet's intent to deliver these plans using an online, interactive tool. The Offeror's proposed solution will be evaluated on the following aspects:

- Readability, navigability, organization, and other pertinent aspects of the user interface design
- Ability to support the objectives outlined in Section J, Attachment J-18, Delivery Mechanism Objectives for State Plans
- Technical design and system adaptability and security

M.4.1.7 Section Seven – Quality Assurance Surveillance Plan

The Offeror will be evaluated on its proposed Quality Assurance Surveillance Plan and the extent to which it accurately monitors and communicates to FirstNet the contractual, operational, financial, and technical performance of the NPSBN.

M.4.1.8 Section Eight – Deliverables Table

The Offeror's proposed deliverables will be evaluated based on its ability to demonstrate industry best practices and professional expertise as well as the alignment with the proposed performance metrics/standards defined in the Offeror's Quality Assurance Surveillance Plan (Section J, Attachment J-9, QASP Surveillance Matrix Template).

M.4.2 Volume II – Coverage and Capacity Factor

The Offeror's proposed solution will be evaluated based on its ability to provide coverage and capacity solutions as described in the sub-factors below. Coverage propagation and geographic information system tools will be utilized to assist in the evaluation process. These tools include but are not limited to MapInfo 11 and ArcGIS. This factor will be evaluated based on both a quantitative and qualitative perspective. The coverage and capacity factor includes evaluation in the following sub-factors:

- Coverage and Capacity Maps and Statistics
- Radio Access Network (RAN) Strategy and Solutions
- IOC Milestones for Coverage and Capacity

M.4.2.1 Coverage and Capacity Maps and Statistics

The Government will evaluate this sub-factor utilizing a quantitative approach. The Offeror's proposed solution will be evaluated for each of the 56 states and territories using the information provided by the Offeror through coverage maps as well as network statistics included in Section J, Attachment J-17,

Coverage and Capacity Template. The Government will evaluate the maps and statistics against the coverage objectives specified in Section J, Attachment J-1, Coverage and Capacity Definitions. For the coverage maps, each individual grid block will be assessed for meeting the definition of coverage (see Section J, Attachment J-1, Coverage and Capacity Definitions). Only those grid blocks that have a reasonable amount of coverage will be considered acceptable. As noted in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.2.1.2.2, Network Planning and Design, detailed site locations are not required; however, for evaluation purposes, the Government reserves the right to request detailed site information (to include all site data for up to two counties per state or territory.) If requested, these data are to be supplied using the "Site Summary" tab in Section J, Attachment J-17, Coverage and Capacity Template.

The Government will evaluate the Offeror's proposed solution using a quantitative approach for each of the following coverage and capacity elements, which are of equal importance:

- **Non-Band 14 Area Coverage** – The amount of land mass that is covered with non-Band 14 coverage solutions
- **Non-Band 14 Population Coverage** – The amount of population that is covered with non-Band 14 coverage solutions
- **Band 14 Area Coverage** – The amount of land mass that is covered with Band 14 coverage solutions
- **Band 14 Population Coverage** – The amount of population that is covered with Band 14 coverage solutions
- **Band 14 Network Capacity** – The amount of designed network capacity for first responders and secondary users

M.4.2.2 RAN Strategy and Solutions

The Offeror's proposed solution will be evaluated qualitatively based on the proposed RAN design solution, which must include architecture, functionality, design, implementation, roadmap, and operational strategies that effectively use resources, skillsets, an organizational structure, and tools.

M.4.2.3 IOC Milestones for Coverage and Capacity

The Offeror's proposed solution will be evaluated qualitatively based on the proposed approach to meeting and/or exceeding the deployment schedule in accordance with the coverage and capacity milestones as provided in Section J, Attachment J-8, IOC/FOC Target Timeline.

M.4.3 Volume II – Products and Architecture Factor

The Offeror's solution will be evaluated based on its proposed approach, including innovation, creativity, and thoroughness, shown in planned execution of the overall objectives as stated in Section C, SOO, and associated Section J attachments as applicable. The products and architecture factor includes evaluation of the Offeror's proposed solution in the following sub-factors:

- Services
- Applications
- Device Ecosystem
- Architecture and Infrastructure
- Operations
- Security
- Test Strategy

M.4.3.1 Services

M.4.3.1.1 Basic Network Services

The Offeror will be evaluated based on its proposed solution to enable basic network services, including but not limited to messaging, streaming services, voice telephony, machine-to-machine, Next Generation 9-1-1, lawful intercept, Wireless Emergency Alerts, and basic data for the NPSBN. The Offeror should outline its approach based on each of the IOC/FOC milestones and compliance with 3GPP or relevant international standards.

M.4.3.1.2 Quality of Service, Priority, and Preemption

The Offeror will be evaluated on its proposed solution for Quality of Service, Priority, and Preemption (QPP) and service readiness in the event of an emergency and/or network congestion. The Offeror will be evaluated on its proposed solution (including systems, interfaces, and settings) pertaining to QPP states (static, dynamic, controlled), Covered Leasing Agreement (CLA) user-states (free range, restricted, pre-empted), emergency states (user type and role), QPP profiles and static user data (default and emergency QPP profiles for different users with different roles), dynamic data (user location, user operational status, incident role, incident identifier, incident location, and incident severity), QPP application profiles, group of application profiles into operational profiles for an agency, dynamic QPP management, and end-to-end Quality of Service and Priority for public safety users. The Offeror will be evaluated on its proposed solution of a dynamic controller.

M.4.3.1.3 Identity, Credential, and Access Management

The Offeror will be evaluated based on its proposed solution pertaining to Identity, Credential, and Access Management (ICAM) within the following elements:

- **Federated Identity Management** – The Offeror's ability to support federated identity management, allowing users of one agency to access data and services provided by a different agency, including evaluation of the proposed federated identity interfaces that the solution supports and any impacts on an existing agency's infrastructure and legacy applications that an agency exposes.
- **Identity Proofing and Onboarding** – The Offeror's ability to support agencies being properly onboarded to leverage the FirstNet ICAM solution, including identifying proofing of users and ensuring the agency is in compliance with security parameters (additional details available in Section J, Attachment J-10, Cybersecurity). The Offeror's proposed timelines and processes for onboarding and certifying an agency and identity-proofing users will be considered. This will include the proposed process for addressing agencies that lack a compliant identity proofing and onboarding solution/process (i.e., Identity-as-a-Service).
- **Credential Management** – The Offeror's ability to support credential management, including ensuring credentials are secure and align with the specifications in Section J, Attachment J-4, System and Standard Views, including but not limited to the management of user attributes and access policies that enable interoperability between agencies.
- **Single Sign On and Authentication** – The Offeror's ability to support effective, efficient, realistic, and secure methods for public safety users to authenticate, including but not limited to authentication into devices, mobile applications, Web applications, and desktop applications.
- **Authorization** – The Offeror's ability to support dynamic access management and the manner in which its solution will easily enable applications to authorize users before granting access to the

application or data, including but not limited to how static and dynamic access policies are created, managed, and applied to applications, services, and resources.

M.4.3.1.4 Mission-Critical Services

The Offeror will be evaluated based on its proposed approach regarding the design and plans for mission-critical Push-to-Talk, data, voice, proximity services, and location services for each IOC/FOC milestone, including its compliance with relevant international standards.

M.4.3.2 Applications

The Offeror will be evaluated based on its proposed solution to execute an applications ecosystem, as defined in Section M.4.3.2.1, Applications Ecosystem. This will include demonstrating its ability to provide an applications ecosystem that supports the NPSBN with capabilities and services relevant to public safety. This will include its proposed solution to provide an ecosystem that includes, at a minimum, an evolving portfolio of mobile, enterprise, cloud services, and applications; an applications development platform; a vibrant application developer community; a FirstNet applications store; local control of users, subscriptions, services, and applications; federation of identity management, data, applications, and resource sharing across diverse public safety agencies; Core service and application delivery platforms; data and applications security; and privacy compliance across local, state, regional, tribal, and federal users.

In addition, this sub-factor includes evaluation of the Offeror's proposed solution within the following elements:

- Applications ecosystem
- Offeror-provided applications

M.4.3.2.1 Applications Ecosystem

The Offeror's proposed solution for the applications ecosystem will be evaluated based on the service delivery platform, application development platform, hosting and cloud services, FirstNet applications store, application life-cycle management, developer and application certification, and application security described.

M.4.3.2.1.1 Service Delivery Platform

The Offeror's proposed solution will be evaluated based on its operational capabilities, which includes gateway policy (i.e., authorization, privacy, throttling, and quotas), security, Application Programming Interfaces (APIs) middleware, and transformation to back-end network service platforms. Additionally, this will include the Offeror's proposed approach regarding its ability to orchestrate one or more network services with an application consuming these APIs, as well as for first responders handling responder emergencies and immediate peril events.

M.4.3.2.1.2 Application Development Platform

The Offeror's proposed solution will be evaluated based on how it supports, allows, and facilitates rapid and innovative third-party public safety application development. In addition, the Offeror's roadmap for creating a vibrant application developer community will be evaluated.

M.4.3.2.1.3 Hosting and Cloud Services

The Offeror's proposed solution will be evaluated based on the extent to which its cloud services solution provides the necessary service redundancy, resiliency, and contingency capabilities to ensure service availability. This includes the analysis of proposed offerings for Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions, as well as data analytics, storage services, and analytics platform.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

M.4.3.2.1.4 FirstNet Applications Store

The Offeror will be evaluated based on its solution and demonstrated approach for supporting a FirstNet applications store, including how the applications store provides public safety agencies and users with a cost-effective, easy method to access secure, value-added public safety applications. The evaluation will include assessing a client's ability to search, browse, sort, select, download, purchase, review, and rate applications. The evaluation will include an assessment of the proposed approach for the application developers' registration process, ease of application publishing and management, application version control, and application monetization and settlements methods.

M.4.3.2.1.5 Application Life-Cycle Management

The Offeror's proposed solution will be evaluated based upon its ability to demonstrate knowledge of application life-cycle management processes, including governance, development, deployment, and operations. This will also include an assessment of the proposed approach for how applications are created based on various categories (e.g., mobile, enterprise, desktop), tested, deployed, updated, monitored, and deprecated.

M.4.3.2.1.6 Developer and Application Certification

The Offeror's proposed solution will be evaluated based on its approach to developing a timely and effective solution for certifying application developers and public safety applications as a means to ensure the applications function as expected and are secure, resilient, scalable, and free from malware and unintended behavior. This will include a detailed analysis of the Offeror's approach pertaining to the processes and criteria for certifying application developers and certifying applications. Additionally, the evaluation will include an assessment of the proposed approach for both newly developed and existing public safety applications and how they are handled and certified.

M.4.3.2.1.7 Application Security

The Offeror's proposed solution will be evaluated based on its approach regarding security of the application layer and the data associated with users. This will include an assessment of the proposed solution regarding data protection against unauthorized access and maximizing privacy, data integrity, and data availability in end-to-end scenarios. Additionally, this evaluation will include an assessment of the Offeror's ability to enable the secure coexistence of certified FirstNet and commercial applications on a device. This will include evaluation pertaining to the approach for data and applications security monitoring, alerting, and mitigation for ongoing security operations.

M.4.3.2.2 Offeror-Provided Applications

The Offeror will be evaluated based on its proposed solution for demonstrating its understanding of the effort, including innovation, creativity, and thoroughness of providing the specific applications described below.

M.4.3.2.2.1 Local Control Application

The Offeror's proposed solution will be evaluated for providing direct and indirect control of the NPSBN to Public Safety Entities (PSEs) through local control. Local control is a set of features that allows a PSE to affect direct change over the operational and administrative characteristics of the NPSBN for its users as well as a set of business processes that provides the PSE indirect input into operational aspects of the NPSBN that affect its users. Details can be found in Section L, Instructions, Notices, and Conditions to Offerors or Respondents, Section L.3.2.2.2.2.1, Local Control Application.

M.4.3.2.2.2 Public Safety Entity Home Page

The Offeror's proposed solution for providing a PSE home page will be evaluated. The home page will provide a central point of access to information about the NPSBN as well as to other applications and information, such as the local control application, news and weather information of interest to the PSE, and link(s) to the customer-facing, Web-based portal. Details can be found in Section L, Instructions, Notices, and Conditions to Offerors or Respondents, Section L.3.2.2.2.2.2, Public Safety Entity Home Page.

M.4.3.3 Device Ecosystem

The Offeror's proposed solution pertaining to the device ecosystem will be evaluated based on a robust device portfolio and its roadmap. This will include the proposed approach to provide the necessary certifications and support.

In addition, this sub-factor includes evaluation of the Offeror's proposed solution within the following elements:

- Management of the Universal Integrated Circuit Card (UICC) SIM types that automatically support all partner and roaming network(s) and the life-cycle support of the profile(s). Devices that can operate across multiple networks with a single UICC are preferable.
- Support of a standards-compliant Device Management client.
- Device approval process, including Federal Communications Commission (FCC) certification, Personal Communications Services (PCS) Type Certification Review Board (PTCRB) certification (including the waiver request process), FirstNet's Device Independent Verification and Validation (IV&V), and carrier acceptance for current and future devices.

M.4.3.3.1 Device Portfolio

The Offeror will be evaluated based on its proposed solution for providing a device portfolio and roadmap that supports Section C, SOO, and completion of Section J, Attachment J-11, Device Specification Template. The proposed solution will be evaluated based on the diversity of the portfolio across key device categories, the Offeror's ability to operate securely on the NPSBN and partner networks, and the ability to be interoperable with the FirstNet applications ecosystem. The proposed solution will also be evaluated based on the device ecosystem as a whole, its life-cycle management, and support for a variety of UICC configurations, accessories, a Bring Your Own Device (BYOD) ownership model, and Mobile Device Management (MDM).

M.4.3.3.2 Band 14 Devices

The Offeror's solution will be evaluated on the proposed approach to provide a Band 14-capable device portfolio and roadmap(s), including but not limited to portables, modems, in-vehicle routers, Vehicular Network Systems, and Machine to Machine (M2M) or Internet of Things (IoT) configurations. The Offeror will also be evaluated on the management ecosystem strategy for devices, including device management and application management and security, as well as the portfolio approach based on each IOC/FOC milestone and compliance with 3GPP or other relevant international standards.

M.4.3.3.3 Universal Integrated Circuit Card Management

The Offeror will be evaluated on its proposed solution for the management of the UICC and the life-cycle support of the profile(s). Devices that can operate across multiple networks with a single UICC are preferable.

M.4.3.3.4 Device Management Client

The Offeror will be evaluated on its proposed solution for support of a standards-compliant device management client.

M.4.3.3.5 Device Approval Process

The Offeror's proposed solution will be evaluated based on its demonstrated ability to provide details of its device approval process, including FCC certification, PTCRB certification (including the waiver request process), FirstNet's Device IV&V, and commercial carrier acceptance for current and future devices.

M.4.3.4 Architecture and Infrastructure

The Offeror will be evaluated on its proposed NPSBN network architecture solution comprising the nationwide Core network architecture, state integration plans, transmission systems, and interconnection and interworking.

M.4.3.4.1 Nationwide Core Network Architecture and State Integration

The Offeror will be evaluated on its proposed NPSBN network architecture solution comprising the following areas for each IOC/FOC milestone:

- Logical architecture regarding system and architecture views for all user and control planes for the NPSBN
- Integration of secondary users without impacting public safety users and services
- Services to public safety users
- Key Core network locations used for the NPSBN
- Network specifications, design criteria, service quality, and operational metrics of the Offeror's solution
- Session continuity between the NPSBN and other networks
- Roaming strategy pertaining to support of roaming with other wireless networks
- Integration of roaming partners, ensuring seamless wireless services throughout the coverage footprint for public safety users, to include an outline demonstrating the proposed approach for integration of rural telecommunications providers
- Internet Protocol (IP) address assignments in the NPSBN and interworking with other networks
- Heterogeneous network integration, including the proposed strategy regarding integration of wireless technologies (e.g., Wi-Fi, small cells, distributed antenna solutions) into the NPSBN to form a seamless network implementation and operation

M.4.3.4.2 Transmission Systems Strategy

The Offeror will be evaluated on its ability to provide a transmission systems approach supporting RAN backhaul, backhaul aggregation, and a nationwide backbone transmission system for each IOC/FOC milestone. Specifically, the Offeror will be evaluated on its proposed solution in the following areas:

- RAN backhaul architecture, topology, and synchronization approach for its RAN solution

- RAN backhaul system aggregation transport network approach
- National transmission network approach
- End-to-end security of the transport network
- Routing and Diameter Routing Agent (DRA) approach for the user and signaling plane traffic on the NPSBN
- Transport service prioritization to ensure the integrity of end-to-end services for public safety, specifically with regard to QPP

M.4.3.4.3 Interconnection and Interworking

The Offeror will be evaluated on its ability to provide a solution for the interconnection and interworking required to support a seamless and interoperable NPSBN. Specifically, the Offeror will be evaluated on its proposed solution in the following areas:

- Integration of state-deployed RANs with the NPSBN, including population locations detailing the function for each location at each of the 56 states and territories
- Public Safety Enterprise Network (PSEN) and Public Safety Answering Point (PSAP) integration in accordance with the FOC milestones
- Public Switched Telephone Network (PSTN), Internet Service Provider (ISP), and peering integration in accordance with each IOC/FOC milestone
- Public Land Mobile Network Number (PLMN) and roaming partner integration in accordance with each IOC/FOC milestone

M.4.3.4.4 Public Safety Grade

The Offeror will be evaluated on its proposed solution for ensuring a level of hardening and resiliency within the NPSBN that will be necessary for public safety services, especially in case of operational challenges that are expected during natural and man-made events. Specifically, the Offeror's proposed solution will be evaluated based on the following areas:

- Network reliability related to the Offeror's network design, and support for demonstrating how its solution consistently performs according to its specifications for each IOC/FOC milestone
- Network resiliency in order to maintain the restoration time specified in Section C, SOO, in the face of natural disasters, faults, and other challenges to normal operation for each IOC/FOC milestone
- Network redundancy in order to increase service availability through local and geo-redundancy solutions designed into the NPSBN for each IOC/FOC milestone
- Mitigation of environmental factors that may have an adverse effect on the NPSBN's performance
- Operational management—including preventative and proactive measures for maintenance, disaster support, and new technologies—which results in a continual improvement of network performance, services, and support of public safety users

M.4.3.4.5 Network Implementation

The Offeror will be evaluated on its network implementation solution comprising network integration strategy, design assumptions, naming and numbering strategies, and implementation approach. Specifically, the Offeror's proposed solution will be evaluated based on the following areas:

- Network integration with partner service providers at each IOC/FOC milestone

- Naming and identifying NPSBN network nodes to facilitate seamless network services implementation and operation at each IOC/FOC milestone
- NPSBN design assumptions at each IOC/FOC milestone
- Numbering/addressing schema for public safety devices
- Program approach and schedule for the implementation of the NPSBN, covering all IOC/FOC milestones
- Migration of public safety users from any temporary non-Band 14 network to the NPSBN as soon as the NPSBN is available in a region
- Mobile number portability to ensure public safety users do not change their phone numbers when migrating to the NPSBN

M.4.3.5 Operations

The Offeror's solution will be evaluated based on the proposed design, architecture, and approach regarding an effective and complete operational life-cycle model that is consistent with the Information Technology Infrastructure Library (ITIL®) or other commercial operational and testing plans for all aspects of the NPSBN. This model should include processes needed for day-to-day management of the network, reactive processes around incidents and national events, and proactive processes resulting in continual improvement of service availability. The areas of operations that follow will be evaluated for the Offeror's proposed solution.

M.4.3.5.1 Network and Service Operations

The Offeror will be evaluated on how its managed services in the following areas will meet the stated service availability objectives for the NPSBN, as identified in Section C, SOO, for all services and applications. These areas contain processes that focus on continuous service delivery and proactive operations of the NPSBN. The Offeror will also be evaluated based on its proposed solution for the following areas:

- Systems and processes to identify and resolve service degradation issues
- National Incident Management System (NIMS) processes and interfaces
- Release management processes
- Business continuity/disaster recovery management processes
- Availability management processes
- Change management processes
- Capacity management processes
- National and local support structure for network configuration, maintenance, and monitoring
- Procedures and protocols to support use of deployable assets for natural disasters and major events

M.4.3.5.2 Business and Operational Support Systems

The Offeror will be evaluated on how its business and operational support systems in the following areas will support meeting the stated service availability objective for the NPSBN, as identified in Section C, SOO, for all billing, operational, and provisioning support systems. Each of these areas should contain processes that focus on support of the user life-cycle on the NPSBN. The Offeror's proposed solution will be evaluated based on the following areas:

- Business and Operational Support Systems (B/OSS) infrastructure

- Network and Element Management Systems
- End-user and device provisioning and management systems
- Configuration management systems
- Billing system capability and flexibility in defining new profiles and billing
- Device management systems
- Subscriber management (customer relationship management) systems
- Asset management systems
- Trouble ticketing systems
- Workflow systems
- Data processing
- APIs available to government for creation of automated reports

M.4.3.5.3 Services Management Center

The Offeror's proposed solution will be evaluated based on its ability to provide an NPSBN Services Management Center that is effective in managing the following operational network and service verticals. Each of these areas should contain processes that focus on the surveillance and response of support staff and systems monitoring the NPSBN. The Offeror's proposed solution will be evaluated based on the following areas:

- Operational center(s) of excellence for management and reporting of NPSBN services (integrated into a single management framework)
- Event-based Element and Network Management System
- Appropriate surveillance and technical support staff
- Effective visibility and timely communication of network and service status
- Around-the-clock (24x7x365) visibility and management of network and service status
- Ongoing quality management and improvement framework for meeting and exceeding performance objectives

M.4.3.5.4 Service Availability

The Offeror's solution will be evaluated based on its proposed plan for providing a redundant network designed to operate during natural and man-made disasters necessary to meet the service availability objective in Section C, SOO.

M.4.3.6 Security

The Offeror's solution will be evaluated based on its proposed architecture, operational, and security testing plans for all aspects of the NPSBN.

M.4.3.6.1 Public Safety Security

The Offeror's solution will be evaluated based on its proposed approach as it pertains to usability, mission primacy, operational security, responder safety, reliability, resiliency, Health Insurance Portability and Accountability Act of 1996 (HIPAA) data protection, Criminal Justice Information Services (CJIS) data protection, payment card industry (PCI) data protection, end-to-end protection of data, privacy, authentication, multi-layer security, and public safety data protection.

M.4.3.6.2 Architecture Security

The Offeror's proposed solution will be evaluated based on its approach related to architectural security considerations as depicted in Section J, Attachment J-3, FCC TAB RMTR, 3GPP standards, GSM Association (GSMA) specifications, transport, external interfaces, end-to-end security management and logging, private encryption key management infrastructure (to include policies and practices), fraud prevention and revenue assurance, network address translation (NAT) support, protection between users, signaling storms, rogue or spoofed devices, heterogeneous network support, operational support system, Domain Name System (DNS) security, messaging security, IP Multimedia Subsystems security, business support system, mobile Virtual Private Network (VPN) support, business continuity and disaster recovery, IP infrastructure network elements, security hardening, cybersecurity governance model, cyber supply chain, training, insider threat mitigation, cloud environments, virtualization security, software-defined networking security, and Voice over IP (VoIP) spam. The Offeror's proposed solution will be evaluated based on the following areas pertaining to domains:

- RAN within a state or territory (either FirstNet- or state-deployed)
- Backhaul network (Enhanced Node Base station) to regional aggregation points
- Aggregation network (aggregation of traffic in a region)
- National transport networks (network connections to regional and national Core sites)
- Evolved Packet Core
- Business Support Systems
- Operational Support Systems
- Applications ecosystem
- IMS
- Value-added services
- Messaging services
- PSE network connectivity
- NPSBN cloud environments

M.4.3.6.3 Device Security

The Offeror's proposed solution will be evaluated based on its approach to device security for FirstNet users, including but not limited to secure operating system architecture, authentication of users and applications, embedded applications, MDM and Mobile Application Management (MAM) (PSE-managed whitelist/blacklist), digital signature of the applications, device security, and BYOD to include devices, applications, and/or wearables.

M.4.3.6.4 Applications Security

The Offeror's proposed solution will be evaluated based on its approach to application security, including but not limited to applications ecosystem security, API security, the application software development life-cycle, application security certification, application vulnerability management, application developer certification, user logging, end-to-end application, application-specific port monitoring and validation, application-device security, data loss prevention, and secure application coexistence.

M.4.3.6.5 Identity, Credential, and Access Management Security

The Offeror's proposed solution will be evaluated based on its approach to effectively provide ICAM with federated identify from PSENs, authorization, credentialing, and the following areas related to identity assurance:

- User to device
- Device to network (Long Term Evolution [LTE] authentication)
- Network to application (identity management)
- Network to PSE network (identity management)
- User to application (identity management)
- User to PSE network (identity management)

M.4.3.6.6 Cryptographic Employment

The Offeror's proposed solution will be evaluated based on its approach to mitigate attack vectors against the NPSBN's infrastructure and devices using encryption.

M.4.3.6.7 Public Safety Enterprise Network Security

The Offeror's proposed solution will be evaluated based on its approach to formulate minimum security standards for PSE networks to connect to the NPSBN.

M.4.3.6.8 Cybersecurity Life-Cycle

The Offeror's proposed solution will be evaluated based on its approach to security, including but not limited to identifying vulnerabilities and threats, determining risks arising from threats and vulnerabilities, prioritizing risks to determine which warrant associated controls to address threats or vulnerabilities, specifying and implementing controls to address or mitigate those threats and vulnerabilities, assessing the effectiveness of controls, and monitoring the security of the system.

M.4.3.6.9 Cybersecurity Systems Engineering

The Offeror's solution will be evaluated based on the proposed cybersecurity systems engineering plan and its approach to ensure sustained security for the NPSBN.

M.4.3.6.10 Risk Management

The Offeror's proposed solution will be evaluated based on its approach to address risk management considerations, including but not limited to a Risk Management Methodology that is executed continuously during the system's development life-cycle and during the life of the NPSBN (to include the use of National Institute of Standards and Technology Risk Management Framework and/or the ISO 27000 series). The Offeror's proposed Risk Management Methodology will be evaluated based on the following steps:

- Asset identification
- Risk impact analysis
- Threat assessment
- Risk mitigation
- Security control selection and deployment
- Risk mitigation operations and maintenance

M.4.3.6.11 Cybersecurity Incident Response

The Offeror's solution will be evaluated based on the proposed Cybersecurity Incident Response Plan.

M.4.3.6.12 Security Operations Center

The Offeror's proposed solution will be evaluated based on its approach in supporting the objectives of the security operations center, including but not limited to:

- Situational awareness that includes collecting, maintaining, and sharing information related to threats to network infrastructure, devices, data, and applications
- 24/7/365 cybersecurity monitoring of network infrastructure, devices, data, and applications
- Monitoring and analysis of user, system, and network access
- Assessment of system and data file integrity
- Establishment of the baseline network activity and utilization
- Recognition and analysis of activity patterns that are indicative of an incident or intrusion
- Analysis of logs for abnormal use patterns
- Information sharing and collaboration that integrates and disseminates information throughout the critical infrastructure partnership network
- Processing and posting suspicious activity reports
- Assessment and analysis that evaluates infrastructure data for accuracy, importance, and implications
- Decision support that provides recommendations to partners and FirstNet leadership

M.4.3.6.13 Continuous Diagnostic Monitoring and Mitigation

The Offeror's solution will be evaluated based on the proposed approach to address hardware asset management, software asset management, vulnerability management, configuration settings management, continuous network and system monitoring, and mitigation strategies.

M.4.3.6.14 Cybersecurity Testing and Certification

The Offeror's proposed solution will be evaluated based on its approach related to cybersecurity testing and certification, including but not limited to:

- Testing life-cycle, including verification of security throughout the life-cycle of selection, procurement, integration, and operations support
- Testing methods to include assessment, testing, examination, and interviewing and associated processes and mechanisms to maintain testing results to ensure optimal accuracy and reproducibility
- Individual system validation
- Integrated configuration testing
- Independent applications/services testing for the following areas:
    - New applications at the national level
    - User-developed or state-developed applications
    - Upgrades to currently approved applications
    - Security patches to currently approved and fielded applications

M.4.3.6.15 Network and Configuration Management

The Offeror's proposed solution will be evaluated based on its approach related to network and configuration management, including:

- Network management
  - Configuration management
  - Configuration management planning and management
  - Configuration identification
  - Configuration control
  - Configuration status and accounting
  - Configuration verification and audit
- Vulnerability management
- Patch management
- Centralized security log management
- Security information and event management

M.4.3.6.16 Environmental and Physical Security

The Offeror's proposed solution will be evaluated based on its approach to environmental and physical security, including but not limited to power failure; humidity detection; cabinet door alarms; uninterruptable power supply (UPS) power failure; facility access control; monitoring and recording of activity within a facility to include egress/ingress (business/after hours and in restricted areas); heating, ventilation, and air conditioning (HVAC) failure or degradation; building door alarms; generator failure; low generator fuel; low battery; closed circuit television (CCTV) video surveillance systems; fire/smoke detection sensors; and protection from natural disasters (e.g., lightning/surge protection, water leak detection).

M.4.3.6.17 Information Security and Data Sensitivity

The Offeror's proposed solution will be evaluated based on its approach to information security and data sensitivity, including data in transit and data at rest. The Offeror's approach will be evaluated for its ability to protect, disseminate, and retain data.

M.4.3.7 Test Strategy

The Offeror's response will be evaluated based on its proposed architecture, design, and implementation of the NPSBN infrastructure to support the objectives (detailed in Section C, SOO) and FCC TAB requirements (detailed in Section J, Attachment J-3, FCC TAB RMTR), as well as the Offeror's ability to provide, demonstrate, verify, and measure aspects of the NPSBN test strategy identified but not limited to the areas specified in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.2.3, Test Strategy.

M.4.4 Past Performance Factor

The Offeror's proposed solution will be evaluated based on the following areas:

- History of successful completion of projects, especially those of similar size and/or scope, history of producing high-quality reports and other deliverables, and history of staying on schedule and within budget

- Quality of cooperation within the Offeror's organization and quality of cooperation and performance between the Offeror's organization and its customers
- Quality of service and improvement, as represented by the past performance data, and the approach to implementing performance measures and for improving system effectiveness over time
- Responsiveness to customers, as represented by past performance data, and success in responding to requests—both scheduled and ad hoc—for services, data, analysis, and additional tasks in a timely and appropriate manner
- Prior historical working relationship between the Offeror and the proposed subcontractors/teaming partners

In accordance with FAR 15.305(a)(2)(iv), in the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available via other sources, the Offeror may not be evaluated favorably or unfavorably as it relates to past performance.

M.4.5 Volume III – Offeror's Value Proposition Assessment

The Offeror's proposed solution will be evaluated based on its ability to meet all objectives, identified in Section C, SOO, and associated attachments in Section J, in exchange for revenues collected from Band 14 enabled public safety users and non-public safety users, use of available budget authority from FirstNet, and any other value-generating opportunities the Offeror can capitalize upon as a result of this contract.

M.4.5.1 Net Present Value of Payments to FirstNet

The NPV calculation of the nationwide (aggregated state and territory and nationwide) payments to FirstNet will be evaluated and utilized in conducting the best value trade-off analysis as described in Section M.3, Basis for Award. The NPV analysis will be conducted utilizing the data provided in the Payments to FirstNet worksheet of the Pricing Template contained in Section J, Attachment J-13. The NPV calculates the current value of a future stream of payments based on a defined interest rate. The Government will evaluate payments above the minimum payment thresholds.

Payments to FirstNet will be discounted to the present value using the 20-year Treasury bond (available at https://www.treasury.gov/resource-center/data-chart-center/interest-rates/Pages/TextView.aspx?data=yield) as published at 5:00 p.m. Eastern Time the day of the release of this RFP.

M.4.5.2 Offeror's Unbalanced and Unreasonable Value Determination

In place of a traditional pricing evaluation, the Government will evaluate the overall value proposition of the Offeror's pricing volume to determine if an unbalanced or unreasonable valuation exists. The overall value proposition is defined as all nationwide elements, which include the gross value, nationwide and state costs, budget authority, and proposed payments to FirstNet and to the Contractor over the life of the contract or in any given year. The Government will evaluate the overall value proposition for each contract year and for each of the 56 states and territories, which may include the aggregate of the entire period of performance (25 years) for the Offeror's proposed overall value proposition. A proposal that is determined to be unbalanced may be rejected if the Government determines that the lack of balance poses an unacceptable risk to the Government. Unbalanced or unreasonable pricing exists where the price of one or more nationwide or state elements is significantly overstated or understated despite an acceptable total overall value proposition.

The Government will perform a cost realism analysis of offers to (1) verify the Offeror's understanding of the requirements, (2) assess the degree to which proposed payments to the Contractor accurately reflect the effort described in the technical volume as it correlates to the IOC/FOC milestones, and (3) identify inconsistencies with specific objectives and associated attachments. The Contracting Officer reserves the right to limit these detailed analyses to proposals that have been evaluated as technically acceptable in Phases II and III of the multi-phased approach.

In addition, this evaluation will assess the proposed approach pertaining to the drawdown of the aggregate total of $6.5 billion of budget authority and the proposed payments to the Contractor for each IOC and FOC milestone, the nationwide Core, and each state and territory RAN, in accordance with the information stated in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.3.2, Payments to the Contractor.

The information provided herein represents the Government's best effort to predict its needs for the objectives identified in this RFP. The Government reserves the right to evaluate any potential risk(s) and may perform a sensitivity analysis based on the overall proposed solution. This analysis may be used to identify and analyze any overall life-cycle expenses the Government would potentially incur as they relate to the proposed solutions for this contract. Any significant risk to the Government resulting from the sensitivity analysis may be reflected in the value proposition assessment. Cost/price risk refers to any aspect of an Offeror's proposal that may have significant negative cost consequences for FirstNet. Where risk is assessed, it may be described in qualitative terms and/or used as a best-value discriminator. The Government reserves the right to limit these detailed assessments to proposals that have been evaluated as technically acceptable in Phases II and III of this multi-phased approach. Additionally, the Government reserves the right to make any adjustment in costs, for evaluation purposes, in order to assess the overall cost to the Government depending on the outcome of the sensitivity analysis based on the proposed solution.

M.4.6 Risk

Each proposal will be assessed to identify potential risk. Risk refers to any aspect of an Offeror's proposal that could have significant negative consequences for the Government. Where risk is assessed, it may be described in qualitative terms and/or used as a best-value discriminator.

Additionally, the Government will assess the relative risks associated with each Offeror's proposal. It is important to note the distinction between proposal risk and performance risk.

- ***Proposal risks*** are those associated with an Offeror's proposed approach in meeting the objectives. Proposal risk is assessed by the proposal evaluators and is integrated into the rating of each specific evaluation factor in the overall evaluation.
- ***Performance risks*** are those associated with an Offeror's likelihood of success in performing the RFP's objectives as indicated by the Offeror's record of past performance. Performance risk is assessed by the proposal evaluators and is assigned a narrative rating in the performance risk (past performance) factor of the evaluation. Additionally, performance risk may be assessed and considered in the rating of each specific evaluation factor in the overall evaluation. The Government may conduct a performance risk assessment based upon the quality of the Offeror's past performance as well as that of its proposed subcontractors (if any), as it relates to the probability of successful accomplishment of the required effort. When assessing performance risk, the Government will focus its inquiry on the past performance of the Offeror and its proposed subcontractors as it relates to all RFP objectives, such as cost, schedule, and

performance, including the Offeror's record of containing and forecasting costs on any previously performed contracts; the Offeror's adherence to contract schedules, including the administrative aspects of performance; the Offeror's history for reasonable and cooperative behavior and commitment to customer satisfaction; and generally, the Offeror's business-like concern for the interests of its customers.

A significant achievement, problem, or lack of relevant data in any element of the work may become an important consideration in the source selection decision. A negative finding under any element may result in an overall high-performance risk rating. Therefore, Offerors are reminded to include all relevant past efforts, including demonstrated corrective actions, in their proposal.

The Offeror's responsibility for award, as defined in FAR 9.104-1, including any special responsibility criteria identified herein will be considered.

M.5 Competitive Range

In accordance with FAR 15.306(c), after evaluating all proposals, if it has been determined to be in the best interest of the Government to establish a competitive range, the Government reserves the right to limit the competitive range for purposes of efficiency. The Government may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated technical proposals (10 U.S.C. 2305(b)(4) and 41 U.S.C. 253b(d)).

The competitive range will be comprised of the most highly rated technical proposals and those Offerors whose proposals have a reasonable chance of being selected for award. The competitive range determination is a qualitative judgment based on the factual content contained in the technical volumes.

Offerors are reminded that if the Contracting Officer determines that the number of proposals that would otherwise be in the competitive range exceeds the number at which an efficient competition can be conducted, the Contracting Officer may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated proposals. The Contracting Officer will promptly notify Offerors of any decision to exclude them from the competitive range.

M.6 Evaluation Support

The Government intends to use unbiased and conflict-free outside contractors to assist in the evaluation of proposals. These contractors will have access to any and all information contained in the Offeror's proposal and may participate in oral presentations and/or technical demonstrations if conducted, and will be subject to appropriate conflict of interest, standards of conduct, and confidentiality restrictions.